PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-202719
(43)Date of publication of application : 19.07.2002

(51)Int.Cl. G09C 1/00
G06F 12/14

(21)Application number : 2001-066850
(22)Date of filing : 09.03.2001

(71)Applicant : SONY CORP
(72)Inventor : SAKO YOICHIRO
FURUKAWA SHUNSUKE
INOGUCHI TATSUYA
KIHARA TAKASHI

(30)Priority
Priority number : 2000337307 Priority date : 06.11.2000 Priority country : JP

(54) DEVICE AND METHOD FOR ENCIPHERINGDEVICE AND METHOD FOR DECIPHERINGAND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a device and a method for enciphering which enable carrying out of a chain of enciphering without necessitating data or random numbers in a special area for an initial value and have high confidentiality natureand to provide a device and method for deciphering and a storage medium. SOLUTION: When data on contents are enciphered and recordedthe data on contents are divided into blocks and the blocks are chained in a chain-like status and enciphered. The initial value at this time is generated from the contents data itself in its sector. In the case of an MPEG streamthe initial value is generated from unique information on a header. Thusit is not necessary to generate initial value by random numbersetc.and loss of a data area will not occur. Since the contents data change at randomthe confidentiality nature is high. Moreoverthe circuit scale can be kept smallbecause a random number generator and the like is not necessary.

CLAIMS

[Claim(s)]
[Claim 1]According to an initial value generated [above-mentioned]encipher data of the 2nd portion of the above-mentioned contents data as a creating means which generates an initial value according to data of the 1st portion of contents dataand output encryption dataand. An enciphering device provided with a cryptographer stage which enciphers continuously data of a different portion from data of the 1st and 2nd portions of the above-mentioned contents data according to the encryption data concerned outputted.
[Claim 2]The enciphering device according to claim 1 which it has a division means to divide the above-mentioned contents data into a block unit which consists of two or more bitsand the above-mentioned creating means is the block unit divided [above-mentioned]and generated an initial value according to data of the 1st portion within the block concerned.
[Claim 3]The enciphering device according to claim 2 which the above-mentioned cryptographer stage is the block unit divided [above-mentioned]and was made to encipher with a block cipher system.
[Claim 4]The enciphering device according to claim 1 which enciphered the above-mentioned initial value.
[Claim 5]The enciphering device according to claim 1 whose change of data of the 1st portion of the above-mentioned contents data was enabled.
[Claim 6]According to data of the 1st portion of contents datagenerate an initial valueencipher data of the 2nd portion of the above-mentioned contents data according to an initial value generated [above-mentioned]and output encryption dataand. An encryption method which enciphered continuously data of a different portion from data of the 1st and 2nd portions of the above-mentioned contents data according to the encryption data concerned outputted.
[Claim 7]The encryption method according to claim 6 which divides the above-mentioned contents data into a block unit which consists of two or more bitsand generated an initial value by a block unit divided [above-mentioned] according to data of the 1st portion within the block concerned.
[Claim 8]The encryption method according to claim 7 which was made to encipher with a block cipher system by a block unit divided [above-mentioned].
[Claim 9]The encryption method according to claim 6 which enciphered the above-mentioned initial value.
[Claim 10]The encryption method according to claim 6 whose change of data of the 1st portion of the above-mentioned contents data was enabled.
[Claim 11]A decoding device made likecomprising:
Encryption data of a portion which make data of the 1st portion of enciphered contents data into an initial valuedecrypt the 2nd portion of the above from the 2nd piece data and above-mentioned initial value of contents data enciphered [above-mentioned]and the decode data concerned is outputtedand is different from data of the 1st and 2nd portions of the above.
A decoding means which decrypts a portion which is continuously different from data of the 1st and 2nd portions of the above from encryption data before that.

A creating means which generates data of the 1st portion of the above from data of the 1st portion of contents data enciphered [above-mentioned].

[Claim 12]The decoding device according to claim 11 which the above-mentioned contents data is enciphered by a block unit which consists of two or more bitsand the above-mentioned decoding means is the above-mentioned block unitand was made to decrypt with a block cipher system.
[Claim 13]The decoding device according to claim 12 which generated data of the 1st portion of the above from data of the 1st portion of contents data which the above-mentioned creating means is the above-mentioned block unitand was enciphered [above-mentioned].
[Claim 14]The enciphering device according to claim 11 which the above-mentioned initial value was encipheredand decodes the above-mentioned initial value and generated data of the 1st portion of the above.
[Claim 15]Make data of the 1st portion of enciphered contents data into an initial valuedecrypt the 2nd portion of the above from the 2nd piece data and above-mentioned initial value of contents data enciphered [above-mentioned]and output the decode data concernedand. Different encryption data of a portion from data of the 1st and 2nd portions of the aboveA decoding method which decrypts a portion which is continuously different from data of the 1st and 2nd portions of the above from encryption data before thatand generated data of the 1st portion of the above from data of the 1st portion of contents data enciphered [above-mentioned].
[Claim 16]The decoding method according to claim 15 which it is enciphered by a block unit which consists of two or more bitsand the above-mentioned contents data is the above-mentioned block unitand was made to decrypt with a block cipher system.
[Claim 17]The decoding method according to claim 16 which generated data of the 1st portion of the above from data of the 1st portion of contents data enciphered [above-mentioned] by the above-mentioned block unit.
[Claim 18]The decoding method according to claim 15 which the above-mentioned initial value was encipheredand decodes the above-mentioned initial value and generated data of the 1st portion of the above.
[Claim 19]According to data of the 1st portion of contents datagenerate an initial valueencipher data of the 2nd portion of the above-mentioned contents data according to an initial value generated [above-mentioned]and output encryption dataand. A storage which enciphers continuously data of a different portion from data of the 1st and 2nd portions of the above-mentioned contents data according to the encryption data concerned outputtedand memorized data of the above-mentioned contents.
[Claim 20]According to an initial value generated [above-mentioned]encipher the above-mentioned contents data as a creating means which generates an initial value according to data of a predetermined portion of a stream of contents dataand output encryption dataand. An enciphering device provided with a

cryptographer stage which enciphers continuously data of a different portion from the above-mentioned contents data according to the encryption data concerned outputted.
[Claim 21]The enciphering device according to claim 20 which it has a division means to divide the above-mentioned contents data into a block unit which consists of two or more bitsand the above-mentioned cryptographer stage is the block unit divided [above-mentioned]and was made to encipher with a block cipher system.
[Claim 22]The enciphering device according to claim 20 which generated an initial value according to data contained in a portion of a header in the above-mentioned stream.
[Claim 23]The enciphering device according to claim 20 which generated an initial value according to a hour entry included in a portion of a header in the above-mentioned stream.
[Claim 24]The enciphering device according to claim 20 which is contained in a portion of a header in the above-mentioned stream and which generated an initial value according to unique information for every contents.
[Claim 25]A hour entry included in a portion of a header in the above-mentioned streamand the enciphering device according to claim 20 which are contained in a portion of a header in the above-mentioned stream and which generated an initial value according to unique information for every contents.
[Claim 26]The enciphering device according to claim 20 which enciphered the above-mentioned initial value.
[Claim 27]The enciphering device according to claim 20 whose above-mentioned stream is an MPEG stream.
[Claim 28]The enciphering device according to claim 27 whose above-mentioned header is a pack headera packet headeror a file header.
[Claim 29]According to data of a predetermined portion of a stream of contents datagenerate an initial valueencipher the above-mentioned contents data according to an initial value generated [above-mentioned]and output encryption dataand. An encryption method which enciphered continuously data of a different portion from the above-mentioned contents data according to the encryption data concerned outputted.
[Claim 30]The encryption method according to claim 29 which divides the above-mentioned contents data into a block unit which consists of two or more bitsand was made to encipher with a block cipher system by a block unit divided [above-mentioned].
[Claim 31]The encryption method according to claim 29 which generated an initial value according to data contained in a portion of a header in the above-mentioned stream.
[Claim 32]The encryption method according to claim 29 which generated an initial value according to a hour entry included in a portion of a header in the above-mentioned stream.
[Claim 33]The encryption method according to claim 29 which is included in a

portion of a header in the above-mentioned stream and which generated an initial value according to unique information for every contents.
[Claim 34]A hour entry included in a portion of a header in the above-mentioned streamand the encryption method according to claim 29 which are included in a portion of a header in the above-mentioned stream and which generated an initial value according to unique information for every contents.
[Claim 35]The encryption method according to claim 29 which enciphered the above-mentioned initial value.
[Claim 36]The encryption method according to claim 29 whose above-mentioned stream is an MPEG stream.
[Claim 37]The encryption method according to claim 36 whose above-mentioned header is a pack headera packet headeror a file header.
[Claim 38]Decrypt the above-mentioned contents data from contents data enciphered as a creating means which generates an initial value according to data of a predetermined portion of a stream of contents dataand the above-mentioned initial valueand output the decode data concernedand. A decoding device provided with a decoding means which decrypts contents data continuously from encryption data and encryption data before that.
[Claim 39]The above-mentioned contents data is enciphered by a block unit which consists of two or more bits.
The decoding device according to claim 38 which the above-mentioned decoding means is the above-mentioned block unitand was made to decrypt with a block cipher system.

[Claim 40]The decoding device according to claim 38 which generated an initial value according to data in which the above-mentioned creating means is included in a portion of a header in the above-mentioned stream.
[Claim 41]The decoding device according to claim 38 with which the above-mentioned creating means generated an initial value according to a hour entry included in a portion of a header in the above-mentioned stream.
[Claim 42]The decoding device according to claim 38 with which the above-mentioned creating means is included in a portion of a header in the above-mentioned stream and which generated an initial value according to unique information for every contents.
[Claim 43]A hour entry by which the above-mentioned creating means is included in a portion of a header in the above-mentioned streamand the decoding device according to claim 38 which are contained in a portion of a header in the above-mentioned stream and which generated an initial value according to unique information for every contents.
[Claim 44]The decoding device according to claim 38 with which the above-mentioned creating means decrypted the above-mentioned initial value enciphered.
[Claim 45]The decoding device according to claim 38 whose above-mentioned stream is an MPEG stream.
[Claim 46]The decoding device according to claim 45 whose above-mentioned

header is a pack headera packet headeror a file header.
[Claim 47]According to data of a predetermined portion of a stream of contents datagenerate an initial valuedecrypt the above-mentioned contents data from enciphered contents data and the above-mentioned initial valueand output the decode data concernedand. A decoding method which decrypted contents data continuously from encryption data and encryption data before that.
[Claim 48]The decoding device according to claim 47 which the above-mentioned contents data is enciphered by a block unit which consists of two or more bitsand the above-mentioned decoding means is the above-mentioned block unitand was made to decrypt with a block cipher system.
[Claim 49]The decoding device according to claim 47 which generated an initial value according to data in which the above-mentioned creating means is included in a portion of a header in the above-mentioned stream.
[Claim 50]The decoding device according to claim 47 with which the above-mentioned creating means generated an initial value according to a hour entry included in a portion of a header in the above-mentioned stream.
[Claim 51]The decoding device according to claim 47 with which the above-mentioned creating means is included in a portion of a header in the above-mentioned stream and which generated an initial value according to unique information for every contents.
[Claim 52]A hour entry by which the above-mentioned creating means is included in a portion of a header in the above-mentioned streamand the decoding device according to claim 47 which are contained in a portion of a header in the above-mentioned stream and which generated an initial value according to unique information for every contents.
[Claim 53]The decoding device according to claim 47 with which the above-mentioned creating means decrypted the above-mentioned initial value enciphered.
[Claim 54]The decoding device according to claim 47 whose above-mentioned stream is an MPEG stream.
[Claim 55]The decoding device according to claim 54 whose above-mentioned header is a pack headera packet headeror a file header.
[Claim 56]According to data of a predetermined portion of a stream of contents datagenerate an initial valueencipher the above-mentioned contents data according to an initial value generated [above-mentioned]and output encryption dataand. A storage which enciphers continuously data of a different portion from the above-mentioned contents data according to the encryption data concerned outputtedand memorized data of the above-mentioned contents.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This inventionfor example to an optical disc like

CD(Compact Disc) 2. When recording / reproducing the data of contentssuch as audio informationin order to aim at protection of the data of contentsit uses for enciphering and recording data and is related with a suitable enciphering device and methoda decoding devicea methodand a storage.

[0002]

[Description of the Prior Art]In recent yearsdevelopment of an optical disc has been furthered as a mass recording medium. For exampleCD (Compact Disc) in which music information was recordedCD-ROM on which the data for computers is recordedDVD (Digital Versatile Disc or Digital Video Disc) dealing with video informationetc. are known.

[0003]The optical disc quoted here is a read-only disk. These daysthe postscript of data and the rewritable optical disc are put in practical use like CD-R (CD-Recordable) disk and a CD-RW (CD-Rewritable) disk. Development of CD2 grade and various optical discs in which compatibility with the both sides of the double density CDthe usual CD playerand personal computer which raised storage capacity in the same shape as CD is improved is furthered.

[0004]It is apprehensive about the data of the contents recorded on the optical disc being used with the spread of such optical discsreproducing it unjustlyor what was reproduced being sold unjustlyand giving an owner of a copyright a disadvantage. then -- receiving contents data for the purpose of protecting right of an owner of a copyrightwhen recording contents data like audio information or a video data on an optical disc -- encryption processing -- ****** -- things are performed.

[0005]Thusas a cipher system used when recording the data of contents on an optical discblock cipherssuch as DES (Data Encryption Standard) and tripple DEShave been used. DES performs initial transposition (scramble)and by every 32 bitswith 16 keys generated from one 56-bit encryption key in beam datait is a typical common key encryptosystem and it enciphers [nonlinear processing is performed one after anotherit transposes again and] 64 bits (8 bytes) data.

[0006]Howeversince a block cipher like DES has the comparatively short length of a blocka similar block may appear frequently and there is a problem in encryption strength.

[0007]Thenin order to raise encryption strengthit considers using the CBC (Ciphering Block Chaining) method. The CBC method raises encryption strength by making the data enciphered by the block unit chain.

[0008]That isin the CBC methodwhen encipheringEX-OR of this input block data and the data which enciphered the block data in front of one of them is taken and enciphered. When decryptingencryption block data is decryptedEX-OR with the encryption block data before that is takenand the original block data is decoded. Thussince it is enciphered making it chain with front block dataencryption strength can be raised in the CBC method.

[0009]

[Problem(s) to be Solved by the Invention]Thusif it enciphers by the CBC method when recording the data of contents on an optical discencryption strength is

raised and protection of copyright can be aimed at more powerfully. Howeverin the CBC methodin order for there to be no last encryption blockit is necessary to prepare an initial value in the block of the beginning at the time of encipheringin order to encipher making it chain with front block data. Thusas an initial value at the time of enciphering by the CBC methodit is easiest to use a fixed value. Howeverif the fixed value was used as an initial value at the time of enciphering the CBC methodthere is a problem in privacy and high encryption strength cannot be maintained. In order to prepare a fixed value as an initial valueit will be necessary to store the fixed value used as this initial value in somewhere.
[0010]Soto the block of encryptionit is possible to make an initial value from the data of other fields which are not included. For exampleECC (Error CorrectingCode) and medium information for an error correction are included. Since these data is not the data itself which has copyrightit is not necessary to protect it and it is not usually included in the block of encryption. Thenit is possible to make an initial value from the data of other fields like ECC or medium information.
[0011]That isdrawing 25 is the example which made the initial value at the time of enciphering by the CBC method from the data of other fields like ECC or medium information. As shown in drawing 25the input block data Di shall be made into 256 block data to 0-255and 1 block shall be 8 bytes (64 bits).
[0012]Firstthe data from other fields is inputted as the initial value inVby EX-OR gate 501EX-OR of the input block data D0 and the initial value inV is takenthis is enciphered by the key information K in the block enciphering circuit 502and encryption block data ED0 is generated.
[0013]Nextby EX-OR gate 501EX-OR of the input block data D1 and encryption block data ED0 before that is takenthis is enciphered by the key information K in the block enciphering circuit 102and encryption block data ED1 is generated.
[0014]HereafterEX-OR of the input block data Di and encryption block data EDi-1 before that is takenthis is enciphered by the key information K in the block enciphering circuit 502and the encryption block data EDi is generated.
[0015]Thussince an initial value will not turn into a fixed value if the initial value inV is made from ECC or medium informationfor example except the data of a blockprivacy goes up.
[0016]Howeverin this waywhen the initial value inV is made from ECC or medium informationfor example except the data of a blockit is certainly needed for encryption of data other than contents data. For this reasonwhen it becomes impossible to encipher and carry out the data communications only of the contents data and the data of contents is transmittedit will be necessary to certainly send ECC and medium information together.
[0017]It is possible as other methods for generating the initial value at the time of enciphering by the CBC method to generate an initial value with a random number.
[0018]That isas shown in drawing 26it is first put into the value generated by the random number by the block data D0 as an initial value.
[0019]The block data D0 containing this initial value is enciphered by the key

information K in the block enciphering circuit 512and encryption block data ED1 is generated.
[0020]Nextby EX-OR gate 511EX-OR of the input block data D1 and encryption block data ED0 before that is takenthis is enciphered by the key information K in the block enciphering circuit 512and encryption block data ED1 is generated.
[0021]HereafterEX-OR of the input block data Di and encryption block data EDi-1 before that is takenthis is enciphered by the key information K in the block enciphering circuit 512and the encryption block data EDi is generated.
[0022]Howeverin this wayif an initial value is generated with a random numberthe initial value generated by the random number will go into the block data D0and it will no longer be put into contents data by the block data D0. Thereforethe problem that it becomes impossible to put contents data into 2040 of 256 blocks (2048 bytes) to 0-255 of one sectorand a data area cannot use for them effectively arises.
[0023]In order to make it generate an initial value with a random numbera random number generation circuit is needed. In order to improve privacywhat can generate numerals random as a random number is requiredand if such a random number generation circuit is providedthe problem that circuit structure increases will arise.
[0024]Thereforewhen performing a chain of encryptionthe purpose of this invention has unnecessary data and random number of a special field for an initial valueand there is in moreover privacy providing a high enciphering device and methoda decoding devicea methodand a storage.
[0025]Other purposes of this invention have a data area in providing the enciphering device which can be used effectively and a methoda decoding devicea methodand a storagewhen performing a chain of encryption.
[0026]
[Means for Solving the Problem]An invention of Claim 1 enciphers data of the 2nd portion of contents data as a creating means which generates an initial value according to data of the 1st portion of contents data according to a generated initial valueand output encryption dataand. It is the enciphering device provided with a cryptographer stage which enciphers continuously data of a portion in which data of the 1st and 2nd portions of contents data differs according to the encryption data concerned outputted.
[0027]An invention of Claim 6 generates an initial value according to data of the 1st portion of contents dataencipher data of the 2nd portion of contents data according to a generated initial valueand output encryption dataand. It is the encryption method which enciphered continuously data of a portion in which data of the 1st and 2nd portions of contents data differs according to the encryption data concerned outputted.
[0028]An invention of Claim 11 makes an initial value data of the 1st portion of enciphered contents datadecrypt the 2nd portion from the 2nd piece data and initial value of enciphered contents dataand output the decode data concernedand. A decoding means which decrypts a portion which is continuously different from data of the 1st and 2nd portions from different encryption data of a portion from

data of the 1st and 2nd portionsand encryption data before thatIt is the decoding device provided with a creating means which generates data of the 1st portion from data of the 1st portion of enciphered contents data.
[0029]An invention of Claim 15 makes an initial value data of the 1st portion of enciphered contents datadecrypt the 2nd portion from the 2nd piece data and initial value of enciphered contents dataand output the decode data concernedand. A portion which is continuously different from data of the 1st and 2nd portions from different encryption data of a portion from data of the 1st and 2nd portions and encryption data before that is decryptedIt is the decoding method which generated data of the 1st portion from data of the 1st portion of enciphered contents data.
[0030]An invention of Claim 19 generates an initial value according to data of the 1st portion of contents dataencipher data of the 2nd portion of contents data according to a generated initial valueand output encryption dataand. It is the storage which enciphers continuously data of a portion in which data of the 1st and 2nd portions of contents data differs according to the encryption data concerned outputtedand memorized data of contents.
[0031]An invention of Claim 20 enciphers contents data as a creating means which generates an initial value according to data of a predetermined portion of a stream of contents data according to a generated initial valueand output encryption dataand. It is the enciphering device provided with a cryptographer stage which enciphers continuously data of a portion in which contents data differs according to the encryption data concerned outputted.
[0032]An invention of Claim 29 generates an initial value according to data of a predetermined portion of a stream of contents dataencipher contents data according to a generated initial valueand output encryption dataand. It is the encryption method which enciphered continuously data of a portion in which contents data differs according to the encryption data concerned outputted.
[0033]A creating means which generates an initial value according to data of a portion of a stream of contents data predetermined in an invention of Claim 38Decrypt contents data from enciphered contents data and an initial valueand the decode data concerned is outputtedand it is the decoding device provided with a decoding means which decrypts contents data continuously from encryption data and encryption data before that.
[0034]An invention of Claim 47 generates an initial value according to data of a predetermined portion of a stream of contents datadecrypt contents data from enciphered contents data and an initial valueand output the decode data concernedand. It is the decoding method which decrypted contents data continuously from encryption data and encryption data before that.
[0035]An invention of Claim 56 generates an initial value according to data of a predetermined portion of a stream of contents dataencipher contents data according to a generated initial valueand output encryption dataand. It is the storage which enciphers continuously data of a portion in which contents data differs according to the encryption data concerned outputtedand memorized data

of contents.
[0036]Data of contents is blockedand it chains with a chain and is enciphered. And an initial value at this time is generated from the contents data of that sector itself. For this reasonit is not necessary to generate an initial value by random numbers etc.and there is no loss of a data area. Since contents data is changing at randomits privacy is high. It is not necessary to carry out easy [of the random number generator etc.]and circuit structure does not increase.
[0037]The initial value itself generated from contents data is enciphered by other contents data. Contents data used as an initial value can be chosen freely. Therebyprivacy improves.
[0038]In recording an MPEG streamit is generating an initial value using unique information included in a header. Information on a header is uniqueand since SCR and a hour entry like PTS change with timetheir privacy is high. It can transmit maintaining an MPEG streamsince an initial value of encryption was formed using information on a header of an MPEG stream. It is not necessary to carry out easy [of the random number generator etc.]and circuit structure does not increase.
[0039]
[Embodiment of the Invention]Hereafterthis embodiment of the invention is described with reference to Drawings. When recording / playing contents data for exampleCD(Compact Disc) 2in order to aim at protection of datathis invention is used for enciphering the data of contentsand is preferred.
[0040]Drawing 1 shows the composition of the appearance of CD2 which can apply this invention. CD2 is an optical disc 120 mm in diameter like the usual CDfor example. Howeverit is good also as 80 mm in diameter like what is called single CD.
[0041]CD2 is developed in consideration of the compatibility of the existing CD player and both sides with a personal computer. As such CD2 is shown in drawing 1a center hall is established in the centerfield AR1 is provided in the inner circumference sideand field AR2 is further provided in the periphery. The mirror part M1 is formed between field AR1 by the side of inner circumferenceand field AR2 by the side of a peripheryand field AR1 by the side of inner circumference and field AR2 by the side of a periphery are divided into it by this mirror part M1. Lead-in groove field LIN1 is provided in the most inner circumference of field AR1 by the side of inner circumferenceand lead-out field LOUT1 is provided in the outermost periphery. Lead-in groove field LIN2 is provided in the most inner circumference of field AR2 by the side of a peripheryand lead-out field LOUT2 is provided in the outermost periphery.
[0042]Field AR1 by the side of inner circumference is the field where compatibility with the existing CD player was planned. Audio information is recorded on this field AR1 in the same format as the usual CD-DA (CD Digital Audio) so that it can reproduce also with the usual CD player. Encryption to the data of contents is not usually performed so that field AR1 by the side of this inner circumference can be treated like the usual CD-DA. Of coursein order to aim at protection of copyrightalso when enciphering the data recorded on field AR1 by the side of this inner circumferenceit thinks. It may be made to record a video data and data other

than audio information of computer program data etc. on field AR1 by the side of this inner circumference. The data of contents is compressed into field AR1 by the side of this inner circumferenceand it may be made to record on it. [0043]On the other handfield AR2 by the side of a periphery is the field which planned compatibility with a personal computer. Data is recordable on this field AR2 by a double density. Audio information is compressed and recorded on this field AR2for example. It is file-ized so that the MP3 (Mpeg-1 Audio Layer-3) method may be usedfor example and compatibility with a personal computer can be planned as compression technology.
[0044]It is one of the compression technology of three layers specified by MPEG1MP3 divides the output of each zone into a frequency axis by MDCT (Modified Cosine Transform)and after it quantizesit is made to carry out Huffman encoding. By compressing audio information by an MP3 methodstorage capacity is expandableand data can be treated with the same file system as a personal computer. field AR2 [for this reason] by the side of a periphery -- an MP3 method -- ******** -- the data of the contents currently-izing [contents] and recordedMake it move to the hard disk of a personal computerand build a music server in a personal computeror it is made to move to the portable MP3 playback player equipped with a flash memoryand it becomes easy to enjoy music reproduction outside.
[0045]Thuscompatibility with a personal computer is planned and the data of the contents currently recorded on field AR2 by the side of a periphery is easy handling. Howeversince it is carried out outside by the data of the contents currently recorded on field AR2 by the side of this periphery more oftenits a possibility that protection of copyright will no longer be protected is high. For this reasonto the data of the contents recorded on field AR2 by the side of a periphery. In order to restrict a copy and reproductionwhile encryption processing is performedthe copyright management information for managing copy prohibition/permissionthe generation management of a copynumber restrictions of a copyreproduction inhibit/permission and restriction of reproduction frequencyrestriction of regeneration timeetc. is recorded on field AR2 by the side of this peripheryfor example.
[0046]Herealthough the data recorded on field AR2 is file-ized by MP3of coursethe data of the contents recorded on field AR2 is not restricted to the file of MP3. As compression technology of audio informationthe MPEG 2-AAC (Advanced Audio Coding) and ATRAC3 grade other than MP3 is known. It is possible to record various data of not only audio information but a video datastill picture datatext dataa computer programetc. on field AR2. Even if it is data of contents recorded on field AR2as long as it is not necessary to encipherit may record without enciphering[0047]thus -- while CD2 is being able to play with a CD player like the usual CDand using field AR2 by the side of a periphery using field AR1 by the side of inner circumference and it makes it cooperate with a personal computer or a portable player -- data **** -- things are made.
[0048]In such CD2especially this invention enciphers the data of contentsuses it

for record/playingand is suitable for field AR2 by the side of a periphery.
[0049]Drawing 2 is an example of the recorder with which this invention was applied. In drawing 2contents data is supplied to the input terminal 1. Contents data is audio informationfor example. As audio informationPCM data may be sufficient and they may be streamssuch as MP3. It is possible to record various thingssuch as still picture dataprogram data of a gamea video datadata of a web page besides audio informationand a textas contents data. The contents data from this input terminal 1 is supplied to the enciphering circuit 4.
[0050]The key information K is supplied to the input terminal 2. The key information K from the input terminal 2 is supplied to the enciphering circuit 4.
[0051]The enciphering circuit 4 enciphers the contents data from the input terminal 1 using the key information K from the input terminal 2. A block cipher is used as a cipher system. The block cipher is enciphering by making 8 bytes at a time into a unitfor exampleand the enciphering circuit 4 is provided with the blocking circuit. He is trying to raise encryption intensity in this example according to making the data enciphered by the block unit chain. Thusa thing with which the data enciphered by the block unit is made to chain is known as a CBC (Ciphering Block Chaining) method.
[0052]The output of the enciphering circuit 4 is supplied to the error correction code-ized circuit 5. An error correction code is added to the contents data enciphered in the enciphering circuit 4 in the error correction code-ized circuit 5.
[0053]The output of the error correction code-ized circuit 5 is supplied to the modulation circuit 6. In the modulation circuit 6record data is modulated with a predetermined modulation method. The output of the modulation circuit 6 is supplied to the record circuit 7.
[0054]The output of the record circuit 7 is supplied to the optical pickup 8. The record circuit 7 is controlled by the system controller 13. Data is recorded on the optical disc 10 by the optical pickup 8. The optical disc 10 is an optical disc of CD2for example.
[0055]The optical pickup 8 is made radially movable [the optical disc 10]. The tracking servo circuit for irradiating with the laser beam from the optical pickup 8 along the track of the optical disc 10although not illustratedVarious kinds of servo circuitssuch as a focus servo circuit for making the spot of the laser beam from the optical pickup 8 focus on the optical disc 10 and a spindle servo circuit which controls rotation of the optical disc 10are provided.
[0056]The key information K from the input terminal 2 is supplied to the mix circuit 9. The copyright management information R is supplied to the input terminal 3and this copyright management information R rewrites and it is supplied mix circuit 9 via the circuit 11. The output of the mix circuit 9 is supplied to the optical pickup 8 via the record circuit 12. By the optical pickup 8the key information K and the copyright management information R are recorded on the optical disc 10 by the record circuit 12.
[0057]The copyright management information R is information for managing copy prohibition/permissionthe generation management of a copynumber restrictions of

a copyreproduction inhibit/permission and restriction of reproduction frequencyrestriction of regeneration timeetc.for example. When performing the generation management of a copynumber restrictions of a copyand restriction of reproduction frequency and restriction of regeneration timewhenever copy and reproduction are performedit is necessary to rewrite the copyright management information R. Rewriting of this copyright management information R is performed by the rewriting circuit 11.

[0058]About the recording place of the key information K and the copyright management information Rit is possible to record on the lead-in groove and lead-out field of the optical disc 10or to record on the radial direction of a track as wobble data.

[0059]Drawing 3 shows the composition of a reversion system. In drawing 3the record signal of the optical disc 20 is played by the optical pickup 22. The optical disc 20 corresponds with the optical disc 10 in drawing 2and CD2 is used as the optical disc 20for example. The output of the optical pickup 22 is supplied to the demodulator circuit 24 via the playback amplifier 23. The movement toward the optical pickup 22 is controlled by the access control circuit 30 by the basis of control of the system controller 29. A tracking servo circuit for the access control circuit 30 to irradiate with the delivery mechanism of an optical pickupand the laser beam from the optical pickup 22 along the track of the optical disc 20It consists of servo circuitssuch as a focus servo circuit for making the spot of the laser beam from the optical pickup 22 focus on the optical disc 20.

[0060]The output of the demodulator circuit 24 is supplied to the error correction circuit 25. Error correction processing is made in the error correction circuit 25. The output of the error correction circuit 25 is supplied to the decryption circuit 26and the lock management information read circuit 27 is supplied. The output of the lock management information read circuit 27 is supplied to the decryption circuit 26.

[0061]The decryption circuit 26 processes decryption of regenerative data using the key information K read in the lock management information read circuit 27. As mentioned abovein this examplethe CBC method is used as a cipher system. The decryption circuit 26 performs decipherment processing of the code of such a CBC method.

[0062]The output of the decryption circuit 26 is supplied to the regenerative circuit 28. The output of the regenerative circuit 28 is outputted from the output terminal 31. A copy and reproduction are restricted by the copyright management information R read in the lock management information read circuit 27.

[0063]As mentioned abovein this examplethe CBC method is used as a cipher system. That isin a recording systemit is the enciphering circuit 4 and encryption processing is performed by the CBC method to the inputted contents data. And in a reversion systemdecryption processing is performed to the contents data reproduced by the decryption circuit 26.

[0064]Whateversuch as DESAESFEALand MISTYmay be used for a block cipher.

[0065]The intensity of a code is raised in the CBC method according to making

the data enciphered by the block unit chain. In this exampleas shown in drawing 42048 bytes is used as one sector and record/playback of the data to the optical discs 10 and 20 are performed by making this sector into a unit.
[0066]That islet in CD the sub-code block which consists of 98 frames be one sector. The area size of this one sector is 2352 bytesand 2048 bytes has become a data area among those.
[0067]For examplewhen enciphering by a DES method64 bits is processed as 1 block and a 56-bit key is used. For this reasonas shown in drawing 5one sector is an 8-byte (64 bits) unitand is divided into the block of 256.
[0068]And encryption processing is performed by the CBC methodmaking it chain with a previous block in each sector.
[0069]That isin the CBC methodEX-OR of this block data and the data which enciphered the block data in front of one of them is takenand this is enciphered. If encryption processing is completed with the CBC method within one sectorit will be the following sector and encryption processing will be similarly performed by the CBC method.
[0070]Thusthe intensity of a code is raised in this example by using the CBC method. And encryption is performed by the CBC method with each sector. For this reasoneven when reproduction of data becomes impossible by generating of an erroretc.it is lost that that influence is completed within that sector and attains to other sectors.
[0071]And in this embodiment of the inventionthe data of the block in the same sector is used as an initial value. Thusthe loss of a data area is lost by using the data of the block in the same sector as an initial value. In the case of music data or contents data like image datathe value of itself is changing at random. For this reasonwhen the data of contents is usedthe privacy of an initial value is also high.
[0072]When using the data of the block in the same sector as an initial valuethe data itself is not enough as privacy. Thenit is possible to use as an initial value what enciphered the data of the block in the same sector. In this exampleEX-OR of one block data in the same sector and the other block data in that sector is takenand what enciphered this is made into the initial value.
[0073]That isencryption processing is explained using drawing 6 and drawing 7. Drawing 6 shows a process when generating an initial valueand drawing 7 shows a process when performing a block cipher continuously.
[0074]When performing encryption processingas it is shown in drawing 6an initial value is generated first.
[0075]That isas shown in drawing 61 ** Dj of the block data in 1 sector to D0 - D255 is sent to EX-OR gate 101. The function f (Di) of the block data Di except the block data Dj in the same sector is sent to EX-OR gate 101.
[0076]By EX-OR gate 101EX-OR with function [of the block data Dj and block data Di other than the block data Dj] f (Di) is calculated.
[0077]EX-OR with function [of the block data Dj and all the block data Di other than the block data Dj] f (Di)EX-OR with function [of the block data Dj and all the block data Di other than the block data Dj] f (Di) may be sufficientand The

block data DjEX-OR with function [of one block data Di other than the block data Dj] f (Di) may be sufficientand it is good as for how many in the number of the block data Di. The function f (Di) may use anything.
[0078]The output of this EX-OR gate 101 is sent to the block enciphering circuit 102. The output of EX-OR gate 101 is enciphered by the key information K in the block enciphering circuit 102. Therebythe initial value inV is calculated. This value is used also as the data EDj which enciphered the block data Dj.
[0079]Thusif an initial value is calculatedas shown in drawing 7EX-OR of this block data and the data which enciphered the block data in front of one of them will be taken using this initial valueand this will be enciphered. And at the time of the block data Djit is used as block data which the data EDj currently used also as an initial value enciphered.
[0080]That iswhen the input block data Dj used as an initial value is in any of (j= 1-254)encryption is performed as follows.
[0081]Firstby EX-OR gate 111EX-OR of the input block data D0 and the initial value inV calculated by drawing 6 is takenand the output of this EX-OR gate 111 is supplied to the block enciphering circuit 112.
[0082]In the block enciphering circuit 112encryption block data ED0 is calculated from the output of EX-OR gate 111and the key information K.
[0083]NextEX-OR of the input block data D1 and encryption block data ED0 is taken by EX-OR gate 111The output of this EX-OR gate 111 is supplied to the block enciphering circuit 112and encryption block data ED1 is calculated from the output of EX-OR gate 111and the key information K in the block enciphering circuit 112.
[0084]Hereafterencryption block data ED2ED3and -- are called for from the input data D2D3and -- in a similar manner.
[0085]If the input block data D2D3and -- are enciphered and input block data is set to Djthe initial value inV calculated by drawing 6 will be outputted as the encryption block data EDj.
[0086]By EX-OR gate 111again And the input block data DiEX-OR of encryption block data EDi-1 is takenthe output of this EX-OR gate 111 is supplied to the block enciphering circuit 112and the encryption block data EDi is called for from the output of EX-OR gate 111and the key information K in the block enciphering circuit 112.
[0087]The same processing is repeated until the input data D255 is enciphered and encryption block data ED255 is outputted.
[0088]When the input block data Dj used as an initial value is the first block data (j= 0)encryption is performed as follows.
[0089]Firstthe initial value inV calculated by drawing 6 is outputted as encryption block data ED0.
[0090]By EX-OR gate 111 shown in drawing 7and the input block data D1EX-OR gate of encryption block data ED0 (equal to the initial value inV) is takenit is supplied to the block enciphering circuit 112 by the output of this EX-OR gate 111and in the block enciphering circuit 112. Encryption block data ED1 is

calculated from the output of EX-OR gate 111and the key information K.
[0091]The same processing is repeated and encryption block data ED2ED3and -- are called for from the input data D2D3and -- until the input data D255 is enciphered and encryption block data ED255 is outputted hereafter.
[0092]When the input block data Dj used as an initial value is the last block data (j= 255)encryption is performed as follows.
[0093]Firstby EX-OR gate 111 shown in drawing 7EX-OR of the input block data D0 and the initial value inV calculated by drawing 6 is takenand the output of this EX-OR gate 111 is supplied to the block enciphering circuit 112.
[0094]In the block enciphering circuit 112encryption block data ED0 is calculated from the output of EX-OR gate 111and the key information K.
[0095]NextEX-OR of the input block data D1 and encryption block data ED0 is taken by EX-OR gate 111The output of this EX-OR gate 111 is supplied to the block enciphering circuit 112and encryption block data ED1 is calculated from the output of EX-OR gate 111and the key information K in the block enciphering circuit 112.
[0096]Hereafterencryption block data ED2ED3and -- are called for from the input data D2D3and -- in a similar manner. The same processing is repeated until encryption block data ED254 of the input data D254 is calculated.
[0097]If it becomes the last block data D255the initial value inV calculated by drawing 6 will be outputted as encryption block data ED255.
[0098]Nextdecoding processing is explained using drawing 8 and drawing 9. Drawing 8 shows a process when performing a block cipher continuouslyand drawing 9 shows a process when decoding the block data which enciphered the initial value.
[0099]When the input block data Dj used as an initial value is in any of (j= 1-254)decryption is performed as follows.
[0100]Firstas shown in drawing 8encryption block data ED0 and the key information K are sent to the block cipher decoder circuit 121and decoding processing of a code is performed by the block cipher decoder circuit 121.
[0101]The output of the block cipher decoder circuit 121 is sent to EX-OR gate 122. The initial value inV is sent to EX-OR gate 122. This initial value inV is the encryption block data EDj.
[0102]By EX-OR gate 122the output of the block cipher decoder circuit 121 and EX-OR with the encryption block data EDj are takenand the block data D0 is decoded.
[0103]Nextencryption block data ED1 and the key information K are sent to the block cipher decoder circuit 121. A code is decoded by the block cipher decoder circuit 121. The output of the block cipher decoder circuit 121 is sent to EX-OR gate 122.
[0104]Encryption block data ED0 before that is sent to EX-OR gate 122.
[0105]By EX-OR gate 122EX-OR of the output of the block cipher decoder circuit 121 and encryption block data ED0 before that is takenand the block data D1 is decoded.

[0106]Hereafterthe block data D1D2and -- are decoded from encryption block data ED1ED2and -- in a similar manner.
[0107]Thuswhile decrypting the block data D2D3and --when the block data to decode turns into the encryption block data EDj equivalent to an initial valueas shown in drawing 9The encryption block data EDj and the key information K are sent to the block cipher decoder circuit 131and decoding processing of a code is performed by the block cipher decoder circuit 131.
[0108]The output of the block cipher decoder circuit 131 is sent to EX-OR gate 132. The function f (Di) between data other than the block data Dj is sent to EX-OR gate 132.
[0109]By EX-OR gate 132EX-OR with function [between the output of the block cipher decoder circuit 131 and data other than the block data Dj] f (Di) is takenand the block data Dj is decoded.
[0110]If the block data Dj is decodedit will return to drawing 8 and the encryption block data EDi and the key information K will be sent to the block cipher decoder circuit 121. A code is decoded by the block cipher decoder circuit 121. The output of the block cipher decoder circuit 121 is sent to EX-OR gate 122. Encryption block data EDi-1 before that is sent to EX-OR gate 122. By EX-OR gate 122EX-OR of the output of the block cipher decoder circuit 121 and encryption block data EDi-1 before that is takenand the block data Di is decoded.
[0111]Hereafterthe same processing is repeated until encryption block data ED255 is decoded.
[0112]When the input block data Dj used as an initial value is the first block data (j= 0)decryption is performed as follows.
[0113]Firstas shown in drawing 9encryption block data ED0 and the key information K are sent to the block cipher decoder circuit 131and decoding processing of a code is performed by the block cipher decoder circuit 131.
[0114]The output of the block cipher decoder circuit 131 is sent to EX-OR gate 132. In EX-OR gate 132it is the block data D0. The function f (Di) between the data of an except is sent.
[0115]By EX-OR gate 132EX-OR with function [of the output of the block cipher decoder circuit 131 and data other than the block data Dj] f (Di) is takenand the block data D0 is decoded.
[0116]If the block data D0 is decodedas shown in drawing 8encryption block data ED1 and the key information K will be sent to the block cipher decoder circuit 121and decoding processing of a code will be performed by the block cipher decoder circuit 121.
[0117]The output of the block cipher decoder circuit 121 is sent to EX-OR gate 122. The initial value inV is sent to EX-OR gate 122. The initial value inV is encryption block data ED0.
[0118]By EX-OR gate 122the output of the block cipher decoder circuit 121 and EX-OR of encryption block data ED0 are takenand the block data D1 is decoded.
[0119]Nextencryption block data ED2 and the key information K are sent to the block cipher decoder circuit 121. Decryption processing is performed by the block

cipher decoder circuit 121.
[0120]The output of the block cipher decoder circuit 121 is sent to EX-OR gate 122. Encryption block data ED1 before that is sent to EX-OR gate 122.
[0121]By EX-OR gate 122EX-OR of the output of the block cipher decoder circuit 121 and encryption block data ED1 before that is takenand the block data D2 is decoded.
[0122]Hereafterthe same processing is repeated until encryption block data ED255 is decoded.
[0123]When the input block data Dj used as an initial value is the last block data (j= 255)decryption is performed as follows.
[0124]Firstas shown in drawing 8encryption block data ED0 and the key information K are sent to the block cipher decoder circuit 121and decoding processing of a code is performed by the block cipher decoder circuit 121.
[0125]The output of the block cipher decoder circuit 121 is sent to EX-OR gate 122. The initial value inV is sent to EX-OR gate 122. This initial value inV is encryption block data ED255.
[0126]By EX-OR gate 122the output of the block cipher decoder circuit 121 and EX-OR of encryption block data ED255 are takenand the block data D0 is decoded.
[0127]Nextencryption block data ED1 and the key information K are sent to the block cipher decoder circuit 121. A code is decoded by the block cipher decoder circuit 121. The output of the block cipher decoder circuit 121 is sent to EX-OR gate 122.
[0128]Encryption block data ED0 before that is sent to EX-OR gate 122.
[0129]By EX-OR gate 122EX-OR of the output of the block cipher decoder circuit 121 and encryption block data ED0 before that is takenand the block data D1 is decoded.
[0130]Hereafterthe block data D2D3and -- are decoded from encryption block data ED2ED3and -- in a similar manner.
[0131]From encryption block data ED254if the block data D254 is decodedas shown in drawing 9encryption block data ED255 and the key information K will be sent to the block cipher decoder circuit 121and decoding processing of a code will be performed by the block cipher decoder circuit 131.
[0132]The output of the block cipher decoder circuit 131 is sent to EX-OR gate 132. The function f (Di) between data other than the block data Dj is sent to EX-OR gate 132.
[0133]By EX-OR gate 132EX-OR with function [between the output of the block cipher decoder circuit 131 and data other than the block data Dj] f (Di) is takenand the block data D255 is decoded.
[0134]Although all also of a chainan initial valueand key information are processed at 64 bits in the above-mentioned example128 bits or 256 bits may be sufficient.
[0135]Drawing 10 - drawing 12 are flow charts which show processing when enciphering and recording data as mentioned above. In this processingone sector which consists of 2048 bytesfor example is enciphered by CBC. one sector -- 8 bytes (64 bits) -- each time -- it is divided into the block of 256.

[0136]In drawing 10one of the block data D0 equivalent to one sector (for example2048 bytes) - the D255 block data Dj is read first (Step S1). And EX-OR with function [of the block data Di] f (Di) is enciphered by the key information Kand the initial value inV is generated (Step S2). This initial value inV is saved (Step S3).
[0137]And it is judged whether the block data Dj used for making an initial value is the first block data (j= 0) (step S4).
[0138]If it is (j= 0)the initial value inV is read (Step S5)and this initial value inV is set to encryption block data ED0 of the block data D0 (Step S6). Encryption block data ED0 calculated is saved (Step S7).
[0139]The number i of block data is initialized by (i= 1) (Step S8). The initial value inV is read (equal to the encryption block data D0) (step S9)and the block data D1 is read (Step S10). EX-OR of the initial value inV and the block data D1 is enciphered by the key information Kand encryption block data ED1 of the block data D1 is generated (Step S11). This encryption block data EDi is saved (Step S12). And (i= 2) **********s the number i of block data (Step S13).
[0140]If it **********s the number i of block dataencryption block data EDi-1 will be read (Step S14)and the block data Di will be read (Step S15). EX-OR of encryption block data EDi-1 and the block data Di is enciphered by the key information Kand the encryption block data EDi of the block data Di is generated (Step S16). This encryption block data EDi is saved (Step S17). And it **********s the number i of block data (Step S18).
[0141]If it is judged whether block number i amounted to "256" (Step S19) and block number i does not amount to "256"a return is carried out to Step S14. And if the same processing is repeatedthe encryption block data EDi is called forand block number i amounts to "256" and is called for to the block data D255processing will be ended until block number i amounts to "256."
[0142]If the block data Dj used for making an initial value from step S4 is not the first block data (j= 0)as shown in drawing 11it will be judged whether the block data Dj used for making an initial value is the last block data (j= 255) (Step S20).
[0143]If it is (j= 255)block number i is initialized by (i= 0) (Step S21). And the initial value inV calculated at Step S2 is read (Step S22)and the block data D0 is read (Step S23). EX-OR of the initial value inV and the block data D0 is enciphered by the key information Kand encryption block data ED0 of the block data D0 is generated (Step S24). This encryption block data ED0 is saved (Step S25). And (i= 1) **********s the number i of block data (Step S26).
[0144]If it **********s the number i of block dataencryption block data EDi-1 will be read (Step S27)and the block data Di will be read (Step S28). EX-OR of encryption block data EDi-1 and the block data Di is enciphered by the key information Kand the encryption block data EDi of the block data Di is generated (Step S29). This encryption block data EDi is saved (Step S30). And it **********s the number i of block data (Step S31).
[0145]If it is judged whether block number i amounted to "255" (Step S32) and block number i does not amount to "255"a return is carried out to Step S27. And

the same processing is repeated and the encryption block data EDi is called for until block number i amounts to "255."
[0146]If a block number is set to "255"the initial value inV calculated at Step S2 will be read (Step S33). And this initial value inV is set to encryption block data ED255 (Step S34)and is saved (Step S35)and processing is ended.
[0147]It is judged not to be the first block data (j= 0) by the block data Dj used for making an initial value from step S4and at Step S20. If it is judged that it is not the last block data (j= 255)eitheras shown in drawing 12the number i of block data will be initialized by (i= 0) (Step S36). The initial value inV calculated at Step S2 is read (Step S37)and the block data D0 is read (Step S38). EX-OR of the initial value inV and the block data D0 is enciphered by the key information Kand encryption block data ED0 of the block data D0 is generated (Step S39). This encryption block data ED0 is saved (Step S40). And (i= 1) **********s the number i of block data (Step S41).
[0148]If it **********s the number i of block datait will be judged whether it is the number j of the place used for this block number i making an initial value (j=i) (Step S42). If it is not (j=i)encryption block data EDi-1 will be read (Step S43)and the block data Di will be read (Step S44). EX-OR of encryption block data EDi-1 and the block data Di is enciphered by the key information Kand the encryption block data EDi of the block data Di is generated (Step S45). This encryption block data EDi is saved (Step S46). And it **********s the number i of block data (Step S47).
[0149]If it is judged whether block number i amounted to "256" (Step S48) and block number i does not amount to "256"a return is carried out to Step S42.
[0150]At Step S42if it is judged that it is (j=i)the initial value inV calculated at Step S2 will be read (Step S49)and let this initial value inV be the encryption block data EDj of the block data Dj (Step S50). This encryption block data EDj is saved (Step S51). And it progresses to Step S47.
[0151]And the same processing is repeated until block number i amounts to "256." Processing will be endedif block number i amounts to "256" and the encryption block data to the block data D255 is called for.
[0152]Nextprocessing when decoding a code is explained. Drawing 13 - drawing 16 are flow charts which show the processing in the case of decoding a code.
[0153]In drawing 13 - drawing 16it is judged whether block number j used as an initial value is (j= 0) (Step S101).
[0154]Encryption block data ED0 is read at the time of (j= 0) (Step S102). This encryption block data ED0 is decoded by the key information Kand the block data D0 is generated by EX-OR of this decoded value and function f (Di) (Step S103). This block data D0 is saved (Step S104).
[0155]Block number i is initialized by (i= 1) (Step S105). Encryption block data ED1 is read (Step S106). And encryption block data ED0 is read (Step S107). Let encryption block data ED0 be the initial value inV (Step S108).
[0156]Encryption block data ED1 is decoded by the key information KEX-OR of this decoded value and initial value inV (equal to encryption block data ED0) is

takenand the block data D1 is generated (Step S109). The generated block data D1 is saved (Step S110). And (i= 2) **********s block number i (Step S111).
[0157]The encryption block data EDi is read (Step S112). Encryption block data EDi-1 is read (Step S113). The encryption block data EDi is decoded by the key information KEX-OR of this decoded value and encryption block data EDi-1 is takenand the block data Di is generated (Step S114). This block data Di is saved (Step S115). And it **********s block number i (Step S116).
[0158]If it is judged whether block number i amounted to "256" (Step S117) and block number i does not amount to "256"a return is carried out to Step S112. The same processing is repeated until block number i amounts to "256." Processing will be endedif block number i amounts to "256" and is decoded to the block data D255.
[0159]If it is judged at Step S101 that block number j used as an initial value is not (j= 0)as shown in drawing 14it will be judged whether block number j used as an initial value is (j= 255) (Step S118).
[0160]If it is (j= 255)block number i is initialized by (i= 0) (Step S119). Encryption block data ED0 is read (Step S120). Encryption block data ED255 is read (Step S121). Let encryption block data ED255 be the initial value inV (Step S122).
[0161]Encryption block data ED0 is decoded by the key information KEX-OR of this decoded value and initial value inV is takenand the block data D0 is generated (Step S123). The generated block data D0 is saved (Step S124). And (i= 1) **********s block number i (Step S125).
[0162]The encryption block data EDi is read (Step S126). Encryption block data EDi-1 is read (Step S127). The encryption block data EDi is decoded by the key information KEX-OR of this decoded value and encryption block data EDi-1 is takenand the block data Di is generated (Step S128). This block data Di is saved (Step S129). And it **********s block number i (Step S130).
[0163]If it is judged whether block number i amounted to "255" (Step S131) and block number i does not amount to "255"a return is carried out to Step S126. The same processing is repeated until block number i amounts to "255."
[0164]If block number i amounts to "255" and processing to the block data D254 is completedencryption block data ED255 will be read (Step S132). This encryption block data ED255 is decoded by the key information Kand the block data D255 is generated by EX-OR of this decoded value and function f (Di) (Step S133). This block data D255 is saved (Step S134)and processing is ended.
[0165]If it is judged at Step S101 that it is not (j= 0) and it is judged at Step S118 that it is not (j= 255)as shown in drawing 15block number i will be initialized by (i= 0) (Step S135).
[0166]Encryption block data ED0 is read (Step S136). The encryption block data EDj is read (Step S137). Let the encryption block data EDj be the initial value inV (Step S138).
[0167]Encryption block data ED0 is decoded by the key information KEX-OR of this decoded value and initial value inV is takenand the block data D0 is generated (Step S139). The generated block data D0 is saved (Step S140). And as shown in

drawing 16(i= 1) **********s block number i (Step S141).
[0168]If it **********s the number i of block datait will be judged whether it is the number j of the place used for this block number i making an initial value (j=i) (Step S142).
[0169]If it is not (j=i)the encryption block data EDi will be read (Step S143). Encryption block data EDi-1 is read (Step S144). The encryption block data EDi is decoded by the key information KEX-OR of this decoded value and encryption block data EDi-1 is takenand the block data Di is generated (Step S145). This block data Di is saved (Step S146). And it **********s block number i (Step S147).
[0170]If it is judged whether block number i amounted to "256" (Step S148) and block number i does not amount to "256"a return is carried out to Step S142.
[0171]If it is judged at Step S142 that it is (i=j)the encryption block data EDj will be read (Step S149). This encryption block data EDj is decoded by the key information Kand the block data Dj is generated by EX-OR of this decoded value and function f (Di) (Step S150). This block data Dj is saved (Step S151). And it is advanced to Step S147.
[0172]And the same processing is repeated until block number i amounts to "256." Processing will be endedif block number i amounts to "256" and decoding to the block data D255 is completed.
[0173]It may always be made a fixed place and may enable it to change about the block data Dj which enciphered the initial value. Privacy can be raised by what change of the block data Dj which enciphered the initial value is enabled for.
[0174]As mentioned abovein this inventionthe initial value in the case of performing block encryption continuously is generated from the contents data itself. For this reasonsince contents data is changing at randomits privacy is high [there is no loss of a data areaand].
[0175]That issince it is the data obtained by sampling case [whose contents data is / like music data]it can be said in itself that it is the randomization-ized data. It is dramatically difficult to get to know which level the value of the music data at a certain time is. Thereforeif an initial value is made from the contents data itselfprivacy will improve similarlyhaving used the random number as an initial value.
[0176]Nextthe case where an MPEG stream is recorded is explained as data of contents.
[0177]As shown in drawing 1the optical disc of CD2 has field AR1 by the side of inner circumferenceand field AR2 by the side of a peripheryand the audio information file-ized by the MP3 method is recorded on field AR2. An MP3 method is one of three layers of the audio information used by MPEG1. Thereforewhen recording the data of MP3 on field AR2 by the side of a peripheryrecord of data is performed based on an MPEG stream.
[0178]As for the stream of MPEGa stream comprises the upper layer (a program layera pack layer) and a low order layer (packet layer). That isat an MPEG streamthe sequence of one program consists of two or more packsandgenerallyeach pack comprises two or more packets. A pack header is

provided in the head of each pack. A packet consists of a packet header and data.
[0179]In CDthe block which consists of 98 frames is used as a sectorand data is recorded by making this sector into a unit.
[0180]Drawing 17 shows a data structure when an MPEG stream is recorded to CD. As shown in drawing 172048 bytes of data area is established in one sector of CD. In 2048 bytes of this data areathe pack and packet of an MPEG stream are arranged in principle at one sector. As shown in drawing 18a file header is provided in the head of a file. An author's management information is arranged at this file header.
[0181]As shown in drawing 17a pack header is provided in the head of one sector. This pack header consists of 14 bytesfor example. A pack start codeand SCR (System Clock Reference) and the bit rate are contained in this pack header.
[0182]A packet header is provided following a pack header. This packet header consists of 18 bytesfor example. A packet start codestream IDPES (Packetized Elementary Stream) header lengthand PTS (Presentation Time Stamp) are contained in this packet header.
[0183]The data (for examplecompressed audio information) of the contents compressed into 2016 bytes of the remainder of one sector with the MPEG system is arranged.
[0184]Thusthe file of MPEG like MP3 is included in the stream of composition of consisting of a pack and a packet. And as shown in drawing 18a file header is provided in the head of a file. The management information of an author like the files ID and ISRC (International Standard Recoding Code) is included in this file header. ISRC is a code of 12 figures which consists of musica companya sound recording yeara recording numberetc. are numbered at the time of the master tape of the musicor creation. It may be made to provide disk ID which can identify the very thing for a disk.
[0185]Thuswhen recording the stream of MPEG on CDa pack and the data of a sector are recorded on the data area of 2048 bytes of one sector in principle. A thing to be enciphered is 2016 bytes of data among the data of these 1 sectorand the encryption of 14 bytes of pack header and 18 bytes of packet header is unnecessary.
[0186]Drawing 19 shows the composition of the block in the case of enciphering the data of the contents of the MPEG stream for one sector. As mentioned aboveit is 2016 bytes of data which needs to be enciphered among the data of one sector in the case of an MPEG stream. Thereforewhen enciphering an MPEG streamas shown in drawing 19the data of one sector is an 8-byte (64 bits) unitand is divided into the block of 252. And EX-OR of this block data and the data which enciphered the block data in front of one of them is taken like the above-mentionedand it is enciphered by the CBC method which is enciphered.
[0187]An initial value is required to encipher by the CBC method. He is trying to generate an initial value from the contents data of the block in the same sector in the above-mentioned example.In the case of an MPEG stream as well as thisan initial value may be made from the contents data of the block in the same sector

itselfbut it may be made to make the initial value of CBC from the header of an MPEG stream paying attention to the unique nature of the header of an MPEG stream.

[0188]That isas shown in drawing 17the pack header and the packet header are provided in the MPEG stream. As shown in drawing 18a file header is provided in the head of a file. It is possible to generate an initial value from these headers.

[0189]For examplethe management information of copyright like ISRCetc. are recorded on the file header. The management information of this copyright is a unique value for every contents. That in case there is a disk header can put a unique value into a disk header for every disk like the serial number of a disk. Such information is unique information for every disk.

[0190]As for the pack headera pack start codeand SCR and the bit rate are contained. In thisSCR is a hour entry for proofreading STC (System TimeClock) used as the standard of a system. A packet start codestream IDPES header lengthand PTS are contained in the packet header. In thisPTS is a hour entry used as a reproductive standard. Since SCR of a pack header and PTS in a packet header change with timethey serve as a unique value.

[0191]The initial value in the case of enciphering by the CBC method is generable using the unique information included in such a header of the MPEG stream.

[0192]When generating the early stages of the CBC method using unique information in the header of an MPEG streamthe information on a header may be used as it isbut privacy is not enough if the information on a header is used as it is.

[0193]Thenit is possible to generate an initial value from the information on the header of some MPEG streamsor to encipher the information on a headerand to generate an initial value. Specificallythe following methods can be considered.

[0194]Firstit is possible to generate an initial value combining the unique information on a file header like copyright informationand the information which changes with time like SCR of a pack headeror PTS in a packet header by a predetermined function.

[0195]Drawing 20 is an example of the process in the case of generating an initial value in this way from the unique information on a file header like copyright informationand the information which changes with time like SCR of a pack headeror PTS in a packet header. In drawing 20the unique information on a file header is suppliedand SCR of a pack header or PTS in a packet header is supplied to EX-OR gate 201. By EX-OR gate 201EX-OR of the unique information on a file headerand SCR of a pack header or PTS in a packet header is calculated. The initial value inV is calculated from the output of this EX-OR gate 201.

[0196]Nextit is possible to encipher the unique information on a file header like copyright informationor the information which changes with time like SCR of a pack headeror PTS in a packet headerand to generate an initial value.

[0197]Drawing 21 A is an example of the process in the case of enciphering the unique information on a file header like copyright informationand generating an initial value. In drawing 21 Athe unique information on a file header is supplied to the enciphering circuit 211. In the enciphering circuit 211the unique information on

this file header is encipheredand the initial value inV is calculated from the output of the enciphering circuit 211.
[0198]Drawing 21 B is an example of the process in the case of enciphering the information which changes with time like SCR of a pack headeror PTS in a packet headerand generating an initial value. In drawing 21 BSCR of a pack header or PTS in a packet header is supplied to the enciphering circuit 221. In the enciphering circuit 221SCR or PTS is enciphered and the initial value inV is calculated from the output of the enciphering circuit 221.
[0199]It is possible to encipher the information searched for from the unique information on a file header like copyright informationand the information which changes with time like SCR of a pack headeror PTS in a packet headerand to generate an initial value.
[0200]Drawing 22 is an example of the process in the case of enciphering further the unique information on a file header like copyright informationand the information which changes with time like SCR of a pack headeror PTS in a packet headerand generating an initial value. In drawing 22the unique information on a file header is suppliedand SCR of a pack header or PTS in a packet header is supplied to EX-OR gate 231. By EX-OR gate 231EX-OR of the unique information on a file headerand SCR of a pack header or PTS in a packet header is calculated. The output of this EX-OR gate 231 is supplied to the enciphering circuit 232. In the enciphering circuit 232the output of EX-OR gate 231 is enciphered and the initial value inV is calculated from the output of the enciphering circuit 232.
[0201]Drawing 23 is an example of the encryption process in the case of enciphering an MPEG stream. In drawing 23by EX-OR gate 301-0EX-OR of the input block data D0 and the initial value inV calculated from the MPEG header is takenand the output of this EX-OR gate 301-0 is supplied to the block enciphering circuit 302-0.
[0202]In the block enciphering circuit 302-0encryption block data ED0 is calculated from the output of EX-OR gate 311and the key information K.
[0203]By EX-OR gate 301-1nextthe input block data D1EX-OR of encryption block data ED0 is takenit is supplied to the block enciphering circuit 302-1 by the output of this EX-OR gate 301-1and in the block enciphering circuit 302-1. Encryption block data ED1 is calculated from the output of EX-OR gate 301-1and the key information K.
[0204]Hereafterthe input data D2D3--encryption block data ED2 from D251ED3--ED251 are calculated in a similar manner.
[0205]Drawing 24 is an example of the decryption process in the case of decoding an MPEG stream. In drawing 24encryption block data ED0 and the key information K are sent to the block cipher decoder circuit 401-0and decoding processing of a code is performed by the block cipher decoder circuit 401-0.
[0206]The output of the block cipher decoder circuit 401-0 is sent to EX-OR gate 402-0. The initial value inV is sent to EX-OR gate 402-0. This initial value inV is the encryption block data inV.
[0207]By EX-OR gate 402-0the output of the block cipher decoder circuit 401-0

and EX-OR with the initial value inV are takenand the block data D0 is decoded.
[0208]Nextencryption block data ED1 and the key information K are sent to the block cipher decoder circuit 401-1. A code is decoded by the block cipher decoder circuit 401-1. The output of the block cipher decoder circuit 401-1 is sent to EX-OR gate 402-1.
[0209]Encryption block data ED0 before that is sent to EX-OR gate 402-1.
[0210]By EX-OR gate 402-1EX-OR of the output of the block cipher decoder circuit 401-1 and encryption block data ED0 before that is takenand the block data D1 is decoded.
[0211]Hereafterthe block data D1D2--D251 are decoded from encryption block data ED1ED2and -- in a similar manner.
[0212]Thuswhen recording an MPEG streamthe initial value in the case of enciphering by the CBC method using an MPEG header can be made using the unique nature of the header of MPEG. Although the initial value is generated using hour entriessuch as SCR of a file headerand a pack header or a packet headeror PTSit may be made to use the information on a disk header further in an above-mentioned example.
[0213]In an above-mentioned examplealthough the data of contents is recorded on the optical disc of CD2as a recording mediumit is not limited to the optical disc of CD2. This invention can be similarly appliedwhen recording the data of contents on CD-DACD-ROM and CD-Ror CD-RW. When recording the data of contents on various recording mediasuch as not only an optical disc but a magnetic diskflash memory cardetc.it can apply similarly.
[0214]When distributing this invention in a network the data of contentseven if it usesit is preferred.
[0215]That isservice which distributes the data of contents like music data using a network has spread in recent years. In such servicein order to aim at protection of the data of contentsto encipher the data of contents is desired. Since the initial value in the case of performing block encryption continuously is generated from the data of the contents data itself or an MPEG stream in this inventionit is convenient also to the encryption in the case of distributing the data of contents.
[0216]
[Effect of the Invention]According to this inventionthe data of contents is blockedand it chains with a chain and is enciphered. And the initial value at this time is generated from the contents data of that sector itself. For this reasonit is not necessary to generate an initial value by random numbers etc.and there is no loss of a data area. Since contents data is changing at randomits privacy is high. It is not necessary to carry out easy [of the random number generator etc.]and circuit structure does not increase.
[0217]According to this inventionthe initial value itself generated from contents data is enciphered by other contents data. The contents data used as an initial value can be chosen freely. Therebyprivacy improves.
[0218]According to this inventionin recording an MPEG streamit is generating the initial value using the unique information included in a header. The information on a

header is uniqueand since SCR and a hour entry like PTS change with timetheir privacy is high. It can transmit maintaining an MPEG streamsince the initial value of encryption was formed using the information on the header of an MPEG stream. It is not necessary to carry out easy [of the random number generator etc.]and circuit structure does not increase.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is an approximate line figure of an example of the optical disc in which this invention was applied.

[Drawing 2]It is a block diagram of an example of the recorder with which this invention was applied.

[Drawing 3]It is a block diagram of an example of the playback equipment in which this invention was applied.

[Drawing 4]It is an approximate line figure showing the composition of a sector.

[Drawing 5]It is an approximate line figure showing the composition of a block.

[Drawing 6]It is a block diagram used for explanation of the encryption processing to which this invention was applied.

[Drawing 7]It is a block diagram used for explanation of the encryption processing to which this invention was applied.

[Drawing 8]It is a block diagram used for explanation of the decoding processing to which this invention was applied.

[Drawing 9]It is a block diagram used for explanation of the decoding processing to which this invention was applied.

[Drawing 10]It is a flow chart used for explanation of the encryption processing to which this invention was applied.

[Drawing 11]It is a flow chart used for explanation of the encryption processing to which this invention was applied.

[Drawing 12]It is a flow chart used for explanation of the encryption processing to which this invention was applied.

[Drawing 13]It is a flow chart used for explanation of the encryption processing to which this invention was applied.

[Drawing 14]It is a flow chart used for explanation of the decoding processing to which this invention was applied.

[Drawing 15]It is a flow chart used for explanation of the decoding processing to which this invention was applied.

[Drawing 16]It is a flow chart used for explanation of the decoding processing to which this invention was applied.

[Drawing 17]It is an approximate line figure used for the explanation in the case of recording an MPEG stream.

[Drawing 18]It is an approximate line figure used for the explanation in the case of recording an MPEG stream.

[Drawing 19]It is an approximate line figure showing the composition of the block in the case of recording an MPEG stream.
[Drawing 20]It is a block diagram used for explanation of the encryption processing to which this invention was applied.
[Drawing 21]It is a block diagram used for explanation of the encryption processing to which this invention was applied.
[Drawing 22]It is a block diagram used for explanation of the encryption processing to which this invention was applied.
[Drawing 23]It is a block diagram used for explanation of the encryption processing to which this invention was applied.
[Drawing 24]It is a block diagram used for explanation of the decoding processing to which this invention was applied.
[Drawing 25]It is a block diagram used for explanation of the conventional encryption processing.
[Drawing 26]It is a block diagram used for explanation of the conventional encryption processing.
[Description of Notations]
4 ... An enciphering circuit26 ... A decryption circuit1020 ... Optical disc